



Juice Shop Update³



German OWASP Day 2023

by **Björn Kimminich** / **@bkimminich**

<https://owasp-juice.shop>

Follow 530

Tweet

Follow @owasp_juiceshop

Follow @bkimminich

Follow @bkimminich

Star 8,217

OWASP JUICE SHOP

OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!



Customer Testimonials



DSCHADOW

The most trustworthy online shop out there.



SHEHACKSPURPLE

The best juice shop on the whole internet!



VANDERAJ

Actually the most bug-free vulnerable application in existence!



<http://owasp-juice.shop>

[@owasp_juiceshop](https://twitter.com/owasp_juiceshop)

JUICE SHOP CTF Extension



The Node package *juice-shop-ctf-cli* helps you to prepare Capture the Flag events with the OWASP Juice Shop challenges for different popular CTF frameworks. This interactive utility allows you to populate a CTF game server in a matter of minutes.

<http://ctf.owasp-juice.shop>



Main selling points

FREE

[http://ebook!
owasp-juice.shop](http://ebook!owasp-juice.shop)



- Free and Open source: Licensed under the MIT license with no hidden costs or caveats
- Easy-to-install: Choose between node.js, Docker and Vagrant to run on Windows/Mac/Linux
- Self-contained: Additional dependencies are pre-packaged or will be resolved and downloaded automatically
- Self-healing: The simple SQLite and MarsDB databases are wiped and repopulated from scratch on every server startup
- Gamification: The application notifies you on solved challenges and keeps track of successfully exploited vulnerabilities on a Score Board
- Re-branding: Fully customizable in business context and look & feel to your own corporate or customer requirements
- CTF-support: Challenge notifications optionally contain a flag code for your own Capture-The-Flag events

<http://owasp-juice.shop> | [@owasp_juiceshop](https://twitter.com/owasp_juiceshop)



Juice Shop Success Pyramid™

Some amazing facts & stats about the project

contributors 95

owasp flagship project

code style standard

openssf best practices gold

test coverage 88%

maintainability A

GitHub ★ 8.2k

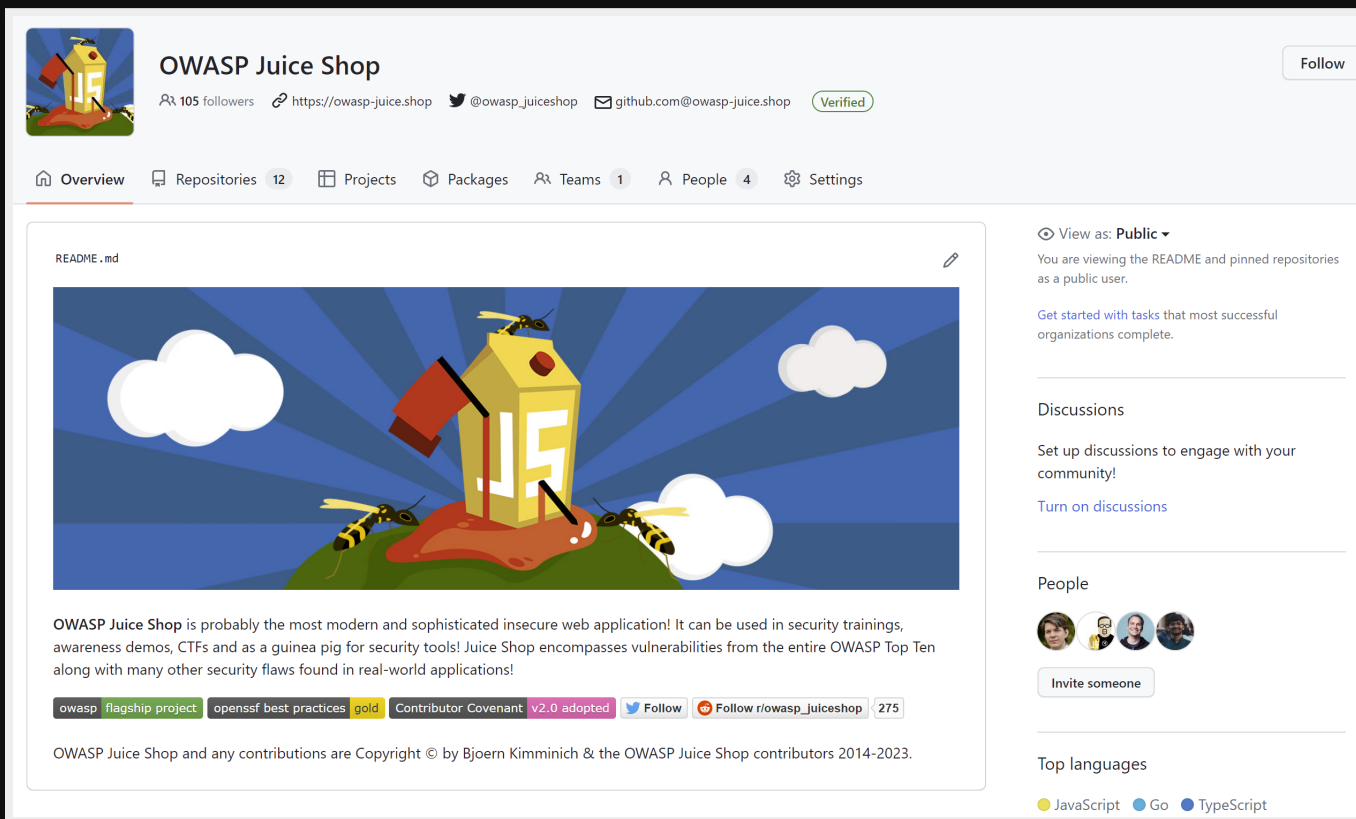
downloads 205k

docker pulls 79M

sourceforge downloads 48k

Official juice-shop GitHub Org

All repos belonging to the project in one place at
<https://github.com/juice-shop>




The screenshot shows the GitHub organization page for OWASP Juice Shop. At the top left is the organization's profile picture, a yellow juice carton with a red flag and a white 'S' on it, sitting on a green globe with bees. To the right of the profile picture is the name 'OWASP Juice Shop', the number of followers '105', and links to the website, Twitter, and email. A 'Follow' button is in the top right corner. Below the profile information is a navigation bar with tabs for Overview, Repositories (12), Projects, Packages, Teams (1), People (4), and Settings. The main content area shows the README for the 'juice-shop' repository. It features the same juice carton logo and a paragraph of text describing the project as a modern and sophisticated insecure web application. Below the text are several badges: 'owasp flagship project', 'openssf best practices gold', 'Contributor Covenant v2.0 adopted', a 'Follow' button, and a 'Follow r/owasp_juiceshop' button with a count of 275. At the bottom of the README section is a copyright notice: 'OWASP Juice Shop and any contributions are Copyright © by Bjoern Kimminich & the OWASP Juice Shop contributors 2014-2023.' On the right side of the page, there is a 'View as: Public' dropdown menu, a note about the public user view, a 'Get started with tasks' link, a 'Discussions' section with a 'Turn on discussions' link, a 'People' section with four profile pictures and an 'Invite someone' button, and a 'Top languages' section with JavaScript, Go, and TypeScript.

OWASP Juice Shop 105 followers <https://owasp-juice.shop> [@owasp_juiceshop](https://twitter.com/owasp_juiceshop) github.com@owasp-juice.shop Verified Follow

[Overview](#) [Repos](#) 12 [Projects](#) [Packages](#) [Teams](#) 1 [People](#) 4 [Settings](#)

README.md



OWASP Juice Shop is probably the most modern and sophisticated insecure web application! It can be used in security trainings, awareness demos, CTFs and as a guinea pig for security tools! Juice Shop encompasses vulnerabilities from the entire OWASP Top Ten along with many other security flaws found in real-world applications!

[owasp flagship project](#) [openssf best practices gold](#) [Contributor Covenant v2.0 adopted](#) [Follow](#) [Follow r/owasp_juiceshop](#) 275

OWASP Juice Shop and any contributions are Copyright © by Bjoern Kimminich & the OWASP Juice Shop contributors 2014-2023.

View as: **Public**

You are viewing the README and pinned repositories as a public user.

[Get started with tasks that most successful organizations complete.](#)

Discussions

Set up discussions to engage with your community!

[Turn on discussions](#)

People

[Invite someone](#)

Top languages

JavaScript Go TypeScript



NEW

Features

from 2020-2023

Coding Challenges

Find code flaw and select appropriate fix for several challenges

Coding Challenge: DOM XSS

Find It Fix It

```
1 filterTable () {
2   let queryParams: string = this.route.snapshot.queryParams.q
3   if (queryParams) {
4     queryParams = queryParams.trim()
5     this.dataSource.filter = queryParams.toLowerCase()
6     this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParams)
7     this.gridDataSource.subscribe((result: any) => {
8       if (result.length === 0) {
9         this.emptyState = true
10      } else {
11        this.emptyState = false
12      }
13    })
14  } else {
15    this.dataSource.filter = ''
16    this.searchValue = undefined
17    this.emptyState = false
18  }
19 }
```

Close Submit

Coding Challenge: DOM XSS

Find It Fix It

Fix 4
Fix 1
Fix 2
Fix 3
Fix 4

Differences (1) Side by Side Line by Line

```
1 1 filterTable () {
2 2   let queryParams: string = this.route.snapshot.queryParams.q
3 3   if (queryParams) {
4 4     queryParams = queryParams.trim()
5 5     this.dataSource.filter = queryParams.toLowerCase()
6 6 -   this.searchValue = this.sanitizer.bypassSecurityTrustHtml(queryParams)
6 6 +   this.searchValue = this.sanitizer.bypassSecurityTrustScript(queryParams)
7 7   this.gridDataSource.subscribe((result: any) => {
8 8     if (result.length === 0) {
9 9       this.emptyState = true
10 10    } else {
11 11      this.emptyState = false
12 12    }
13 13  })
14 14  } else {
```

CSRF	☆☆☆	Change the name of a user by performing Cross-Site Request Forgery from another origin.	Broken Access Control	unsolved
Confidential Document	☆	Access a confidential document.	Sensitive Data Exposure	Good for Demos solved <>
DOM XSS	☆	Perform a DOM XSS attack with <code><iframe src="javascript:alert(`xss`)"></code> .	XSS	Good for Demos solved 🔍 <> 1/2
Database Schema	☆☆☆	Exfiltrate the entire DB schema definition via SQL Injection.	Injection	unsolved <>

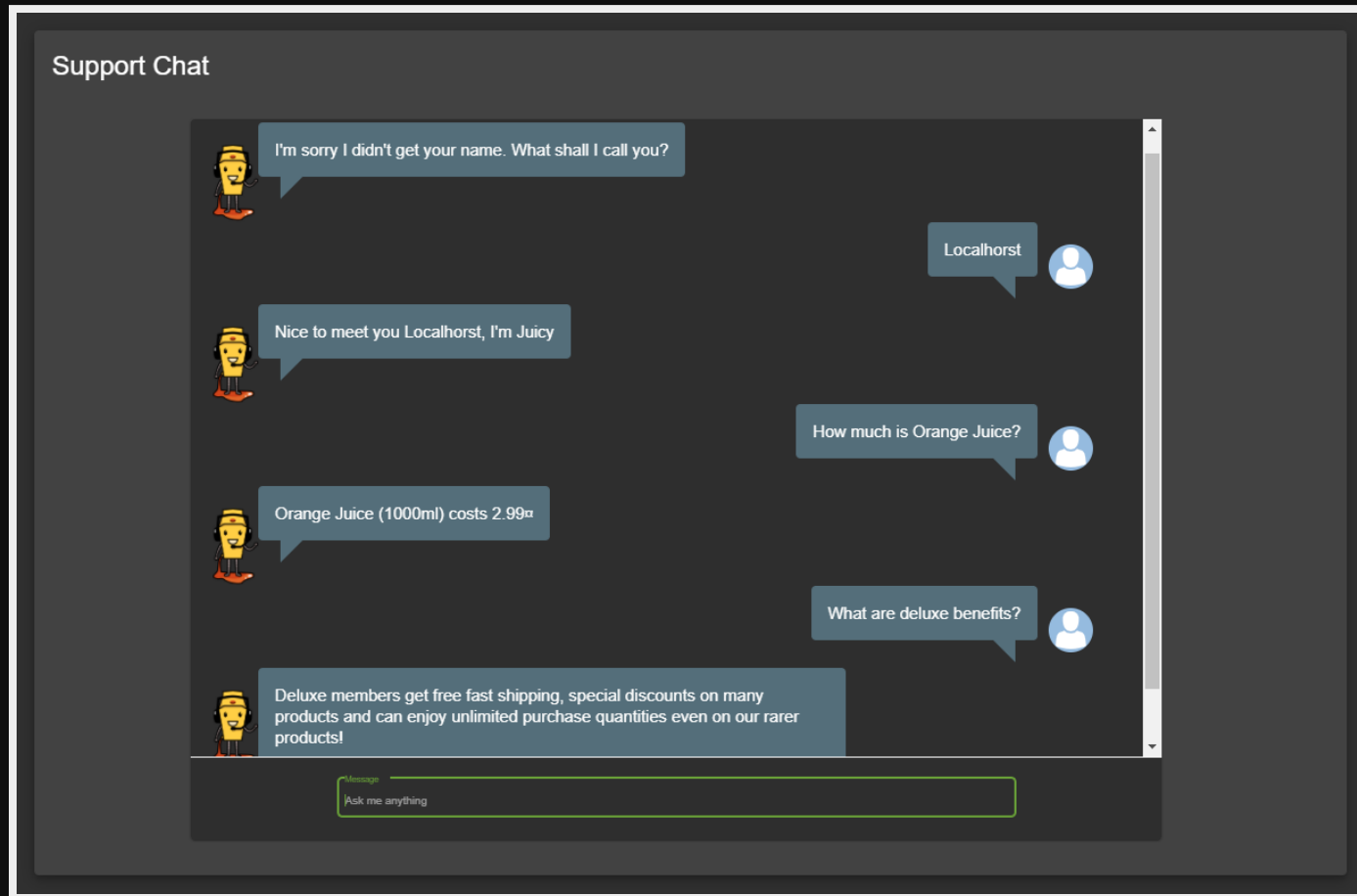
Cheat Detection

Solved challenges are rated based on cheating probability

```
[0] info: Restored 'Fix It' phase of coding challenge localXSSChallenge (DOM XSS)
[0] info: Restored 'Find It' phase of coding challenge scoreboardChallenge (Score Board)
[0] info: Restored 'Fix It' phase of coding challenge scoreboardChallenge (Score Board)
[0] info: Solved 'Find It' phase of coding challenge loginAdminChallenge (Login Admin)
[0] info: Accuracy for 'Find It' phase of coding challenge loginAdminChallenge: 0.5
[0] info: Cheat score for "Find it" phase of loginAdminChallenge solved in lmin (expected ~2min): 0.35365
[0] info: Solved 'Fix It' phase of coding challenge loginAdminChallenge (Login Admin)
[0] info: Accuracy for 'Fix It' phase of coding challenge loginAdminChallenge: 1
[0] info: Cheat score for "Fix it" phase of loginAdminChallenge solved in lmin (expected ~2min): 0.539975
[0] info: Solved 3-star loginJimChallenge (Login Jim)
[0] info: Cheat score for tutorial loginJimChallenge solved in lmin (expected ~3min) with hints allowed: 0.8261666666666667
[0] info: Solved 'Find It' phase of coding challenge loginJimChallenge (Login Jim)
[0] info: Accuracy for 'Find It' phase of coding challenge loginJimChallenge: 0.045454545454545456
[0] info: Cheat score for "Find it" phase of loginJimChallenge solved in lmin (expected ~2min): 0.6848083333333334
[0] info: Solved 'Fix It' phase of coding challenge loginJimChallenge (Login Jim)
[0] info: Accuracy for 'Fix It' phase of coding challenge loginJimChallenge: 0.1
[0] info: Cheat score for "Fix it" phase of loginJimChallenge solved in 0min (expected ~2min): 0.8438749999999999
```

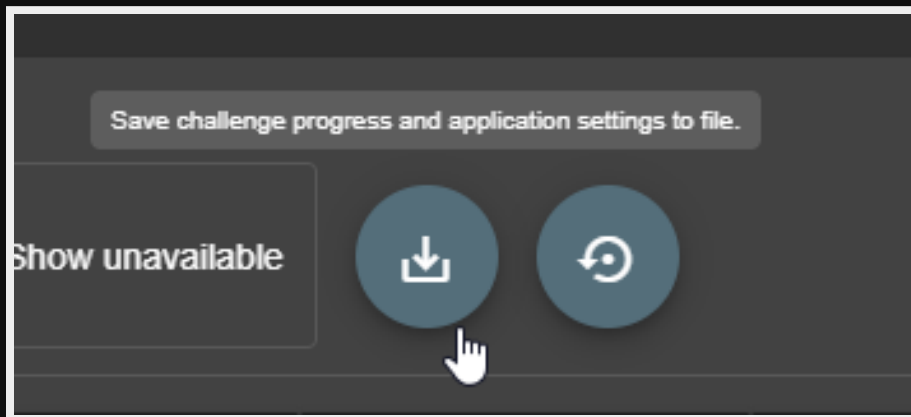

Support Chatbot

Blends NLP, AI and ML into a delicious Turing-Test- 🍹



Local Backup

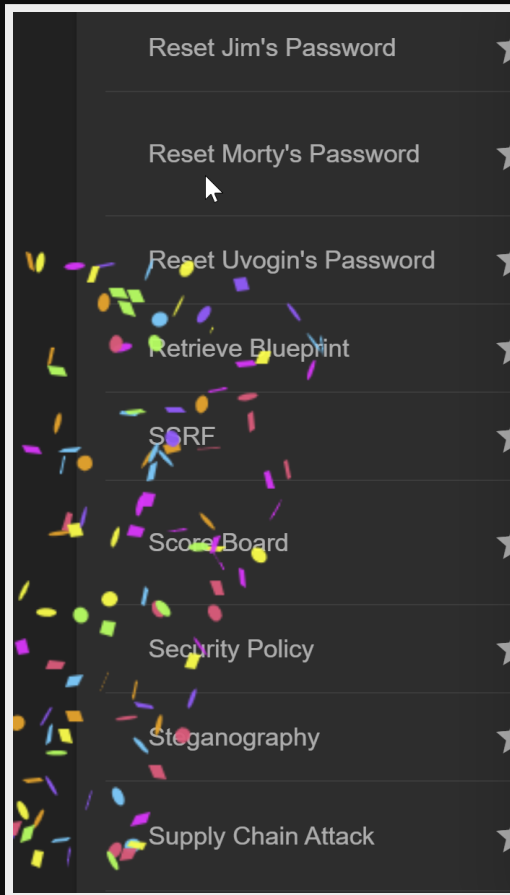
Save and later restore your hacking progress as well as language, Score Board filters, banner dismissal to a JSON file



```
{
  "version": 1,
  "scoreBoard": {
    "displayedDifficulties": [ 1, 2 ],
    "displayedChallengeCategories": [
      "Broken Access Control",
      "Broken Anti Automation"
    ]
  },
  "banners": {
    "welcomeBannerStatus": "dismiss",
    "cookieConsentStatus": "dismiss"
  },
  "language": "de_DE",
  "continueCode": "rzJa4Xpa...57LBN7Xv7o"
}
```

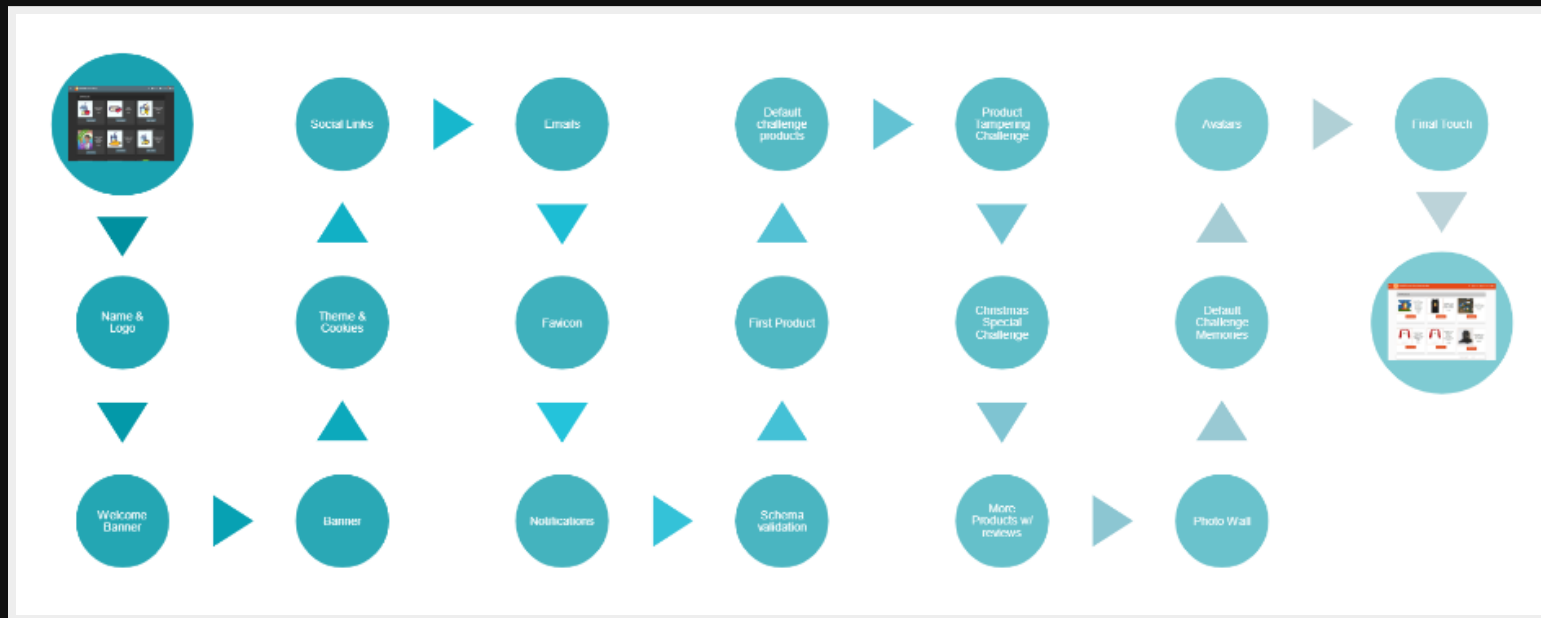
🎆 🎆 Confetti cannon 🎆 🎆

Whenever a challenge is solved, a confetti cannon fires



Official Tutorials

Presentations, snippets and step-by-step guides for advanced topics



- **Customization** - Build a theme in 18 easy steps
- **Integration** - Siphon juicy data in 5 different ways

Solution Webhook

Sends a payload to a specified URL whenever a challenge is solved

```
{
  "solution": {
    "challenge": "localXssChallenge",
    "cheatScore": 0,
    "totalCheatScore": 0.15,
    "issuedOn": "2020-12-15T18:24:33.027Z"
  },
  "ctfFlag": "b0d70dce...b85fac6785dba2349b",
  "issuer": {
    "hostName": "fv-az116-673",
    "os": "Linux (5.4.0-1031-azure)",
    "appName": "OWASP Juice Shop",
    "config": "default",
    "version": "12.3.0-SNAPSHOT"
  }
}
```

Deep links from OpenCRE

OpenCRE v2 will show direct links to Juice Shop hacking challenges as Tool : OWASP Juice Shop training resources

The screenshot shows the OpenCRE v2 search interface. At the top, there is a search bar with the text "Search...", a dropdown menu for "Topic text", and a "Search" button. Below the search bar, the text "Open CRE" is visible on the left. The main content area is divided into two columns. The left column is titled "Results matching : xxe" and "Matching CREs". It contains a single result: "CRE : 764-507 : Restrict XML parsing (against XXE)". The right column is titled "Matching sources". It contains three results: 1. "Standard : ASVS : Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks. : V5.5.2". 2. "Tool : OWASP Juice Shop : xxeFileDisclosureChallenge : XXE Data Access". Below this, there is a reference link: "Reference: https://demo.owasp-juice.shop/#!/score-board?challenge=XXE%20Data%20Access". A note follows: "Tool : OWASP Juice Shop : xxeFileDisclosureChallenge : XXE Data Access is the same as sources:". Below this note is a list of related sources: "CRE : 732-148 : Vulnerability management". 3. "Tool : OWASP Juice Shop : xxeDosChallenge : XXE DoS".

Open CRE

Search... Topic text Search

Results matching : xxe

Matching CREs

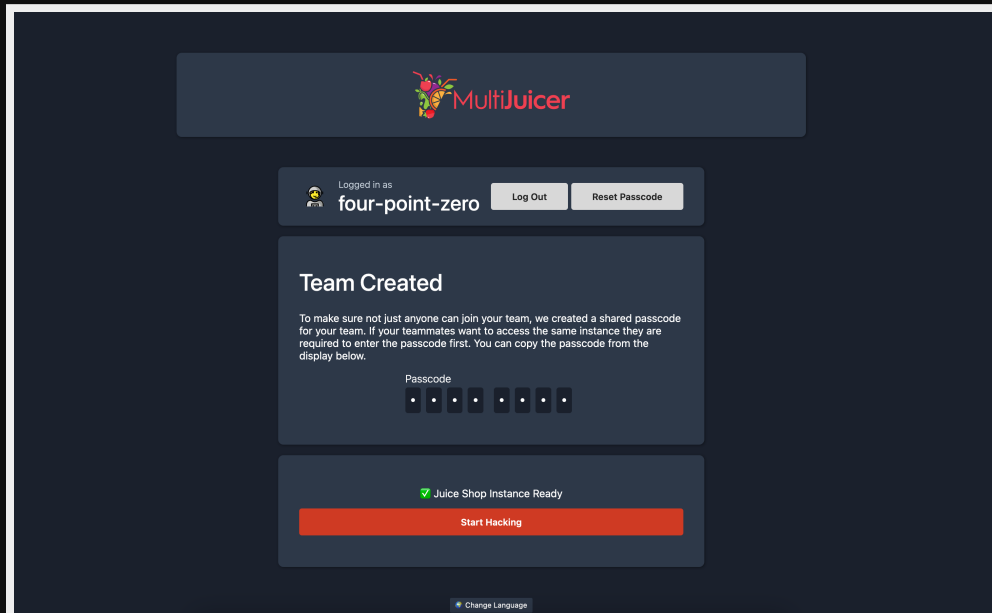
- ▶ CRE : 764-507 : Restrict XML parsing (against XXE)

Matching sources

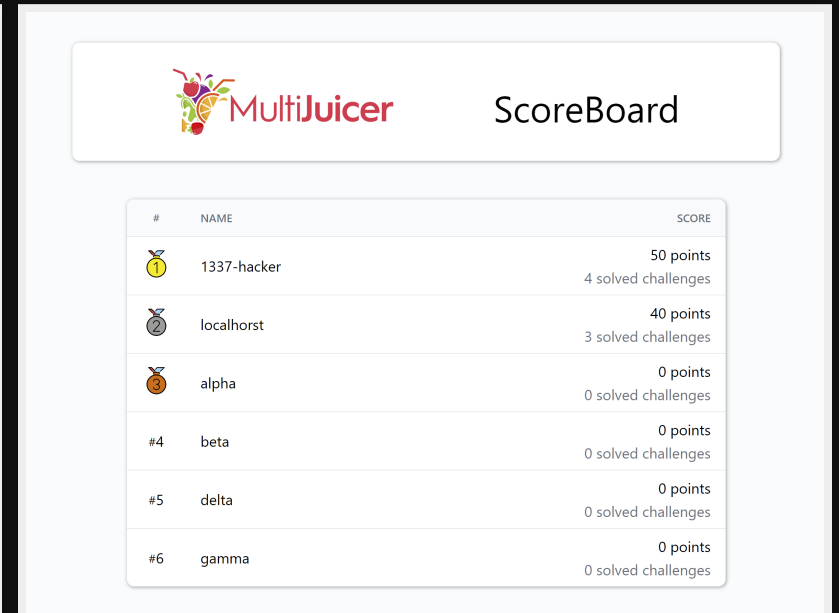
- ▶ Standard : ASVS : Verify that the application correctly restricts XML parsers to only use the most restrictive configuration possible and to ensure that unsafe features such as resolving external entities are disabled to prevent XML eXternal Entity (XXE) attacks. : V5.5.2
- ▼ Tool : OWASP Juice Shop : xxeFileDisclosureChallenge : XXE Data Access
Reference: <https://demo.owasp-juice.shop/#!/score-board?challenge=XXE%20Data%20Access>
Tool : OWASP Juice Shop : xxeFileDisclosureChallenge : XXE Data Access is the same as sources:
 - CRE : 732-148 : Vulnerability management
- ▶ Tool : OWASP Juice Shop : xxeDosChallenge : XXE DoS

MultiJuicer Platform

3rd party multi-user platform now comes with internal Score Board for team events and CTFs



The screenshot shows the MultiJuicer user interface. At the top, the MultiJuicer logo is displayed. Below it, the user is logged in as 'four-point-zero' with 'Log Out' and 'Reset Passcode' buttons. A 'Team Created' message is shown, indicating that a shared passcode has been generated for the team. The passcode is displayed as a series of dots. Below this, a 'Juice Shop Instance Ready' message is shown with a green checkmark, and a red 'Start Hacking' button is visible. At the bottom, there is a 'Change Language' link.

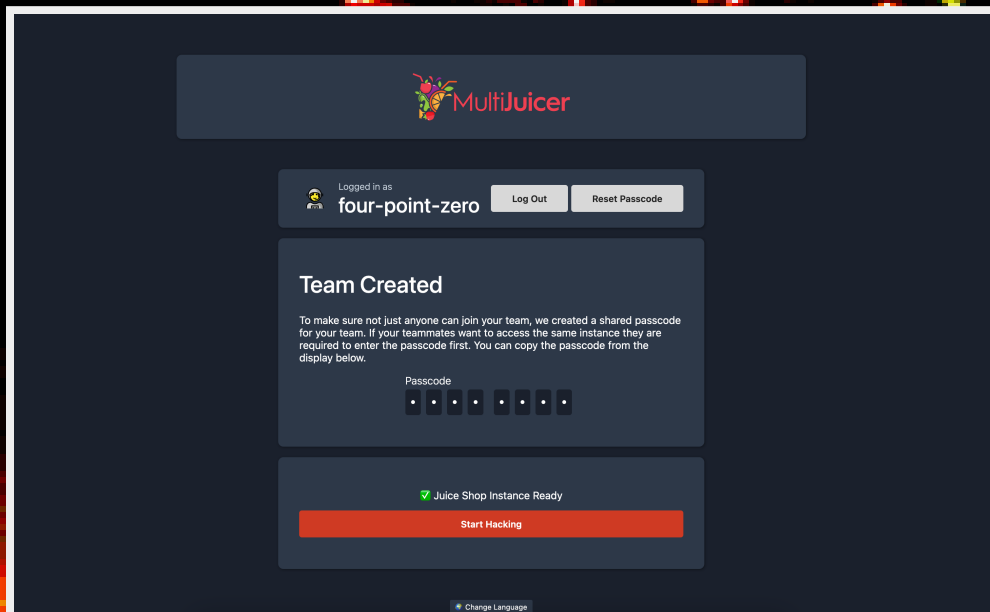


The screenshot shows the MultiJuicer ScoreBoard. The MultiJuicer logo is at the top left, and the title 'ScoreBoard' is at the top right. Below the header is a table listing teams and their scores.

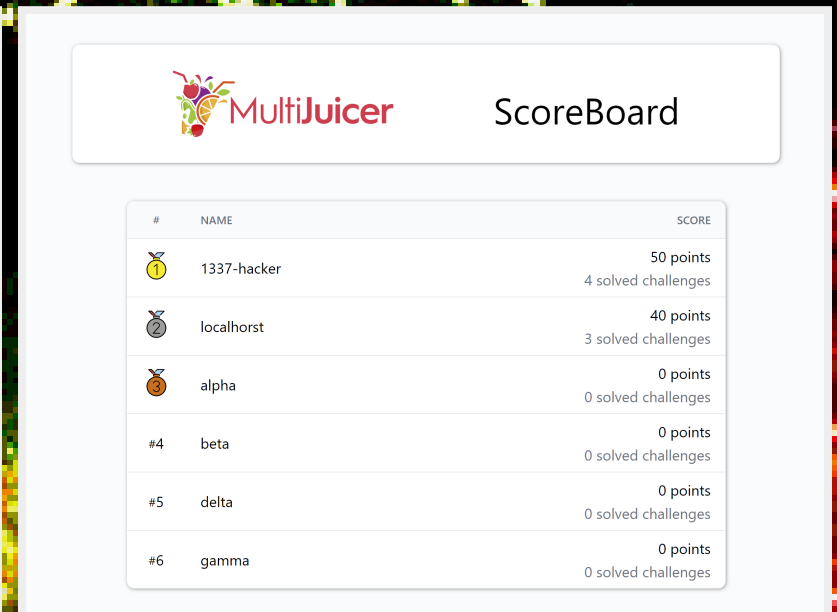
#	NAME	SCORE
1	1337-hacker	50 points 4 solved challenges
2	localhorst	40 points 3 solved challenges
3	alpha	0 points 0 solved challenges
#4	beta	0 points 0 solved challenges
#5	delta	0 points 0 solved challenges
#6	gamma	0 points 0 solved challenges

MultiJuicer Platform

OUR OFFICIAL MULTI-USER PLATFORM now comes with internal
Score Board for team events and CTFs



The screenshot shows the MultiJuicer platform interface. At the top, the MultiJuicer logo is displayed. Below it, the user is logged in as 'four-point-zero' with 'Log Out' and 'Reset Passcode' buttons. A 'Team Created' message is shown, stating that a shared passcode has been generated for the team. The passcode is displayed as a series of dots. Below this, a green checkmark indicates that the 'Juice Shop Instance' is ready, and a red 'Start Hacking' button is visible. At the bottom, there is a 'Change Language' link.



The screenshot shows the MultiJuicer ScoreBoard. At the top, the MultiJuicer logo and the title 'ScoreBoard' are displayed. Below this is a table listing teams and their scores.

#	NAME	SCORE
1	1337-hacker	50 points 4 solved challenges
2	localhorst	40 points 3 solved challenges
3	alpha	0 points 0 solved challenges
#4	beta	0 points 0 solved challenges
#5	delta	0 points 0 solved challenges
#6	gamma	0 points 0 solved challenges

18:15 left for...



Demo

Project Roadmap

Move **Pwning OWASP Juice Shop** eBook away from legacy `gitbook` (GSoC 2023 Project w/ Parth Nanda)

Add Web3 specific hacking and coding challenges (GSoC 2023 Project w/ Rishabh Keshan)

Renovate the Score Board for best possible user experience (Ongoing re-design contract)

Enhance precision of cheat detection with new data sources and algorithms

Bring **overall test coverage** back over 90%+

Sell NFT collection ⇒ ₳ \$UÇE\$\$

Official NFT collection


You thought we were joking, weren't you?


A yellow juice carton character with a smiling face, arms, and legs, standing on a red puddle.

 Juice Shop

Juicy Bot


[BUY THIS ITEM >](#)


A yellow juice carton character wearing a black headset with a microphone, standing on a red puddle.

 Juice Shop

Juicy Chat Bot

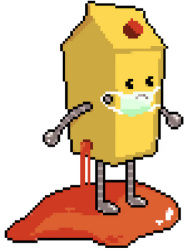
[BUY THIS ITEM >](#)


A black and yellow striped wasp with wings, standing on a red puddle.

 Juice Shop

Juicy Evil Wasp Prev. \downarrow 0.0266

[BUY THIS ITEM >](#)

A yellow juice carton character wearing a light blue surgical mask, standing on a red puddle.

 Juice Shop

Masked Juicy Bot

[BUY THIS ITEM >](#)

Score Board UI/UX re-design

Contracted designer working in close feedback loop w/ Core Team

The screenshot displays the OWASP Juice Shop Score Board interface. At the top, the header includes a hamburger menu, the OWASP Juice Shop logo, a search icon, an account icon, and the language setting 'EN'. The main content area features a dark background with green accents. It shows two '70% ScoreBoard' progress indicators, a '20/106 Problems Solved' counter, and a star rating system with 6/13, 5/14, and 2/9 stars. Below this is a search bar and filter controls for 'Reset Filters', 'DIFFICULTY', 'All', 'STATUS', 'Solved', 'TAGS', and 'Good For Demo'. A series of category buttons are displayed, including 'All', 'Broken Access Control', 'Broken Anti Automation', 'Broken Authentication', 'Cryptographic Issues', 'Improper Input Validation', 'Injection', 'Insecure Deserialization', 'Miscellaneous', 'Security Misconfiguration', 'Security through Obscurity', 'Sensitive Data Exposure', 'Unvalidated Redirects', 'Vulnerable Components', 'XSS', and 'XXE'. The main content area shows a grid of challenge cards, each titled 'XSS Bjoern's Favourite Pet' and featuring a description, a 'Good for Demo' button, a 'Tutorial' button, and a star rating.

🙏 Thank you for your unwavering interest in the project!



Copyright (c) 2023 **Björn Kimminich**

Licensed under the **MIT license**.

Created with [reveal.js](#) - The HTML Presentation Framework

